UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,079	01/22/2004	Daniel Brokenshire	AUS920030972US1	6481

50170 7590 02/28/2008

IBM CORP. (WIP)
c/o WALDER INTELLECTUAL PROPERTY LAW, P.C.
P.O. BOX 832745
RICHARDSON, TX 75083

EXAMINER	
ANWARI, MACEEH	
ART UNIT	**PAPER NUMBER**
2144	

MAIL DATE	DELIVERY MODE
02/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/763,079
Filing Date: January 22, 2004
Appellant(s): BROKENSHIRE ET AL.

Stephen R. Tkacs
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/30/2007 appealing from the Office action mailed 7/31/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 22 and 23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. More specifically, the appellant fails to sufficiently point out or describe computer readable media.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 22-23 each fall under a judicial exception, an abstract idea, and are not directed to a practical application of such a judicial exception because they fail to produce a tangible result.

Furthermore, claims 22 and 23 disclose a computer program product, sharing the same above mentioned components, and failing to fall under one of the statutory categories. It is software per se and fails to provide a tangible result. As the appellant is

attempting to claim a manufacture, the examiner notes that the claim is lacking a proper computer readable medium.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-15 and 18-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Shrader, U.S. Patent No. 6,914,985.

Shrader teaches:

Claim 1:

A system for secure communication, comprising: a random value generator configured to generate a random value (Shrader Col. 11, lines 47-48; teaches this because the enveloped data is constructed and generated at random); a message validation code generator (Shrader Col. 2, lines 19-29 & Col. 13, line 57-67; states that the enveloped data have validation checks) coupled to the random value generator and configured to generate a message validation code based on a predetermined key (Shrader Figure 3 & 4C & 7 & Col. 1, line 27-43; states how the Public-key cryptography standard is applied within his and other inventions), a message (Shrader Col. 2, lines19-40; teaches here that using the PKCS #7 one

would be able to include encrypted messages), and the random value; a one-time pad generator coupled to the random number generator and configured to generate a one-time pad based on the random value and the predetermined key; and a masked message generator coupled to the one-time pad generator and configured to generate a masked message based on the one-time pad and the message (Shrader Col. 11, lines 65-67; meets the limitation of generating a masked message based on the one-time pad by stating that the encrypted content/data be padded to a multiple of some block size); and a transmitter configured to transmit a secure message that comprises the random value, the masked message, and the message validation code to a message target, wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code (Col. 13 lines 57-67).

Claims 2- 4:

Wherein the message validation code generator (MVC), and the one-time pad generator (OTP), employs a first one-way hash function and wherein the MVC employs a first one-way hash function and the OTP employs a second one-way hash function (Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms.)

Claim 5:

The system as recited in claim 1, further comprising a protected message envelope (PME) generator coupled to the random value generator (Col. 11, lines

46-47; meets the limitations of a PME and a random generator), the message validation code generator (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitations of a message validation process), and the masked message generator (Col. 13, lines 34-44; reads on an encryption messaging process), and configured to generate a protected message envelope based on the random value, the message validation code, and the masked message (the combination of the above sections and Figure 3 anticipate all the features within this claim).

Claim 6:

The system as recited in claim 5, wherein the transmitter is coupled to the protected message envelope generator and configured to transmit the protected message envelope to the message target (Col. 13, lines 57-67 & Col. 14, lines 1-7; reads on the limitations of the transmitter and transmission).

Claim 7:

A system in a message target for secure communication, comprising:

a receiver configured to receive a secure message transmitted from a message source, wherein the secure message comprises a protected message envelope;

a protected message envelope reader configured to receive the protected message envelope (Col. 12, lines 4-7 & Col. 15, lines 38-63; meets the limitations of protected message enveloped reader) and extract a random value, a masked message (Col. 11, lines 47-48 & 62-67 & Col. 12, lines 1-3; reads on the random value and the masked message components), and a first message

validation code from the received protected message envelope, wherein the random value, the masked message, and the first message validation code are generated at the message source (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation); a one-time pad generator coupled to the protected message envelope reader and configured to generate a one-time pad based on the random value and a predetermined key (Col. 11, lines 46-67; reads on the limitation of the pad and the key); and a message unmasker coupled to the one-time pad generator and protected message envelope reader, and configured to generate an unmasked message based on the one-time pad and the masked message (Col. 12, lines 4-7& 34-46 & Col. 15, lines 38-63; reads on the unmasking of the masked message)

Claim 8:

The system as recited in claim 7, wherein the one-time pad generator employs a first one-way hash function (Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claim 9:

The system as recited in claim 7, further comprising a validation module (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation) coupled to the protected message envelope reader (Col. 12, lines 4-7 & Col. 15, lines 38-63; meets the limitations of protected message enveloped reader) and the message unmasker (Col. 12, lines 4-7& 34-46 & Col. 15, lines 38-63; reads

on the unmasking/decrypting of the masked/encrypted message), the validation module comprising: a message validation code generator configured to generate a second message validation code based on the predetermined key, the unmasked message(Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation/authentication of the message and the key), and the random value(Shrader Col. 11, lines 47-48; teaches this because the enveloped data is constructed and generated at random); and a message validation code comparator coupled to the protected message envelope reader and the message validation code generator and configured to generate a validation based on the first message validation code and the second message validation code(Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation/authentication).

Claims 10-11:

Wherein the validation module employs a first one-way hash function and wherein the validation module employs a first one-way hash function and the one-time pad generator employs a second one-way hash function (Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claim 12:

A method in a message source for secure communication, comprising: generating a random value (Shrader Col. 11, lines 47-48; teaches this because the enveloped data is constructed and generated at random); generating a

message validation code based on a message, the random value, a predetermined key (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation/authentication and the key), and a first one-way hash function; generating a one-time pad based on the random value (Shrader Col. 11, lines 65-67; meets the limitation of generating a masked message based on the one-time pad by stating that the encrypted content/data could be padded), the predetermined key, and a second one-way hash function; generating a masked message based on the message and the one-time pad; (Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms); and transmitting a secure message that comprises the random value, the masked message, and the message validation code to a message target, wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code (Col. 13 lines 57-67).

Claim 13:

The method as recited in claim 12, further comprising generating a protected message envelope based on the random value, the masked message, and the message validation code (Col. 11, lines 46-67; reads on the limitations of the protected message envelope, the random value along with the masked/encrypted message; Col. 2, lines 19-29 & Col. 13, lines 57-67 meet the limitations of the validation).

Claim 14:

The method as recited in claim 13, wherein the secure message comprises the protected message envelope (abstract).

Claim 15:

Wherein the first one-way hash function and the second one-way hash function are the same one-way hash function (Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claims 16-17:

(Canceled)

Claim 18:

A method in a message target for secure communication, comprising:

receiving a secure message transmitted from a message source, wherein the secure message comprises a random value, a masked message, and a first message validation code (Col. 11, lines 46-67; reads on the limitations of the protected message envelope, the random value along with the masked/encrypted message; Col. 2, lines 19-29 & Col. 13, lines 57-67 meet the limitations of the validation); generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function; and generating an unmasked message based on the one-time pad and the masked message (Shrader Col. 11, lines 65-67; meets the limitation of generating a masked message based on the one-time pad by stating that the encrypted content/data could be padded; Shrader Figure 3 & 4C & 7 & Col. 1, line 27-43 & Col. 12 lines

4-7; reads on the predetermined key limitation and the unmasking/decrypting of the masked/encrypted message).

Claim 19:

The method as recited in claim 18, further comprising: generating a second message validation code based on the unmasked message, the random value (Col. 11, lines 46-48; reads on the limitations of the random values), the predetermined key and a second one-way hash function; and comparing the first message validation code to the second message validation code to determine a validity of the unmasked message (Figures 3 & 4A-B & Col. 2 lines 19-40 & Col. 13 lines 57-67; reads on the limitations of the message validation including the decryption, the key and the hash function).

Claim 20:

The method as recited in claim 19, wherein the first one-way hash function and the second one-way hash function are the same one-way hash function (Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claim 21:

The method of claim 18, wherein the secure message comprises a protected message envelope, the method further comprising: extracting the random value, the masked message, and the first message validation code from the received protected message envelope (Figure 5A-B & Col. 2 lines 19-32;

reads on the limitations the protected message envelope; and reads on the limitations of the message validation).

Claim 22:

A computer program product for secure communications in a message source, the computer program product having a computer readable medium with a computer program embedded thereon (Col. 20 lines 12-23; reads on the medium), the computer program comprising: computer code for generating a random value (Col. 11, lines 46-48; reads on the limitations of the random value); computer code for generating a message validation code based on a message to be sent, the random value, a predetermined key, and a first one-way hash function (Col. 2, lines 19-32 & Col. 11, lines 46-61; reads on the limitations of the random value, the key, and the hash function); computer code for generating a one-time pad based on the random value, the predetermined key, and a second one-way hash function (Col. 11, lines 46-67; reads on the limitations of the padded data, the random value, the key and the hash function); computer code for generating a masked message based on the message to be sent and the one-time pad; computer code for generating a protected message envelope based on the random value, the masked message, and the message validation code (Col. 11, lines 46-67 & Col. 13, lines 57-67; has the limitations of the masked message, the padded data, the protected message envelope, the random value and the message validation); and computer code for transmitting the protected message envelope to a message target, wherein the message

target is configured to unmask the masked message to form the message and validate the message using the message validation code (Col. 13 lines 57-67 and 20 lines 3-11).

Claim 23:

A computer program product for secure communications in a message target, the computer program product having a computer readable medium with a computer program embedded thereon (Col. 20 lines 12-23; reads on the medium), the computer program comprising: computer code for receiving a protected message envelope transmitted from message source; computer code for extracting a random value (Col. 11, lines 46-48; reads on the limitations of the random value), a masked message, and a first message validation code based on the protected message envelope, wherein the random value, the message, and the first message validation code are generated at the message source (Figure 5A-B & Col. 2 lines 19-32; reads on the limitations of receiving the protected message envelope; and by stating that the system allows for recursion, envelope nesting, and the authentication of the content of the message, reads on the limitations of the message validation); computer code for generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function (Col. 11, lines 46-67 reads on the padded data, the random value, the key and the hash function); computer code for generating an unmasked message based on the one-time pad and the masked message (Col. 11, lines 65-67 & Col. 12, lines 4-7; reads on the limitation of the padded data and the

decrypting/unmasking of the message); computer code for generating a second message validation code based on the unmasked message, the random value, the predetermined key, and a second one-way hash function (Col. 2, lines 19-32 & Col. 11 lines 47-48; read on the validation irrespective of number of iterations, also reads on the random factor, the key, and the hash functions); and computer code for comparing the first message validation code to the second message validation code to determine a validity of the unmasked message (Col. 2, lines 19-32; once again read on the validation irrelevant of the number of times the data is authenticated).

(10) Response to Argument

Appellant's arguments filed have been fully considered but are not persuasive. In substance, the appellant argues A) claims 22 and 23, as currently amended, fall under a statutory category; B) none of the cited portions teach a message validation code based on a predetermined key, a message and a random value; C) the message validation code is a separate value that is transmitted with the masked message; D) Shrader does not teach the claimed features arranged as they are in claim 5.

In response to A), although examiner agrees with appellant where "software must be executed on some device or structurally tied to some computer readable medium to realize its function", the claims fail to explicitly meet either of these conditions. Nowhere in the claims, 22 and 23, is it stated that the computer code is "executed". Furthermore the claims are not structurally tied to a tangible

computer readable media. The only reference in the specification appears to be directed to other non-statutory subject matter (i.e. signal, energy, microwave).

In response to B), examiner respectfully disagrees. Shrader discloses a validation code based upon a predetermined key, a message and a random value. The validation code is in part a "digital signature" (Col. 13 lines 57-67). A digital signature is a security mechanism that relies on two keys that are used to encrypt messages before transmission and to decrypt them on receipt. They are also useful in establishing non-repudiation. A digital signature is always generated by using a message and a predetermined key (Col. 11 lines 47-48). The predetermined keys of Shrader are based upon random values. Therefore, the validation code of Shrader is based on a predetermined key, a message and a random value. Therefore Shrader still meets the scope of the limitations as currently claimed.

In response to C), examiner respectfully disagrees. First of all the limitation the *message validation code based on a predetermined key, a message, and a random value* is not clear; because it is does not send anything, neither does it prohibit it from sending anything. The *message validation code* is partially based on a predetermined key, a message and a random value. A digital signature, as stated above, is always generated by using a message and a predetermined key (Col. 11 lines 47-48). Furthermore, in response to appellant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the message

validation code is a separate value, generating a one-time pad based on a key and then masking the message) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to D), examiner respectfully disagrees. The appellant has simply stated structural elements with an intended use. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. Regarding the order with which structural elements are presented, the order of structural elements void of any interaction therewith are not given weight. A mere structural equivalence in the prior art is sufficient to meet the scope of the limitations. A specific order of interaction must be explicitly presented in the claims. Claimed subject matter not the specification is the measure of the invention. Disclosure contained in the specification cannot be read into the claims for the purpose of avoiding prior art. In re Sporck, 55 CCPA 743, 386 F .2d 924, 155 USPQ 687 (1986); In re Self, 213 USPQ 1, 5 (CCPA 1982); In re Priest, 199 USPQ 11, 15 (CCPA 1978).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

M.A. 2/14/2008

Conferees:

William Vaughn (SPE)

John Follansbee (SPE)

/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2144

/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2151

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2144